Remarks

This reply is responsive to the Office communication mailed January 26, 2005. Unless otherwise indicated, page and paragraph references herein are to that communication.

Claim 1 has been amended to recite that the digital secure repository is "associated with said user independently of a particular user device" and stores access rights to the digital content "granted to said user by a provider". Support for the association of the digital secure repository with a user may be found in the sentence bridging pages 16 and 17 of the specification. Support for its device independence may be found, for example, in the final paragraph on page 8 of the specification.

The recitation that the access rights in question are granted to the user by a provider is meant to distinguish the present invention from such mechanisms as parental access controls that are set by the user to limit access by children in his or her household. The "provider" in this case may be any appropriate entity from which the user obtains his rights, such as the rights owner himself or an intermediary such as the administrator of the illustrated content distribution portal.

Claim 6 has been cancelled, since its recitations now appear in claim 1 as amended.

Claim 11 has been similarly amended to recite that the digital secure repository is associated with a user independently of a particular user device and stores access rights to the digital content granted to the user by a provider. This claim has also been amended to incorporate certain other clarifying changes, as has claim 14.

Claim 13 has been amended, primarily as regards punctuation and conjunctions, to emphasize the conditional nature of the steps following the "if" statement. Claim 14 has been similarly amended as regards its two nested "if" statements.

Claim 18 has been amended recite that the information about access rights is read from a digital secure repository of the type claimed in claims 1 and 11. Claim 18 has also been amended to make certain corrections relating to antecedents and the like and to clarify the conditional nature of the steps following the "if" statement.

Claims 26 and 28 have been similarly amended to recite that the digital secure repository is associated with a user independently of a particular user device and stores access rights to the digital content granted to the user by a provider. These claims have also been amended to incorporate certain other clarifying changes.

Finally, new claim 30 is directed to a method of controlling the rendering of digital content to which a user has been granted access rights by a provider. In accordance with the claimed invention, the digital content is stored on a storage device accessible to a user, while the access rights to the digital content are stored in a digital secure repository that is associated with the user independently of a particular user device. The rendering of the digital content on a rendering device is controlled in accordance with the access rights to the digital content stored in the digital secure repository. Dependent claim 31 is directed to a computer program product.

Specific groups of claims based upon particular independent claims are discussed below.

Claims 1-10

Claim 1 as amended is directed to a framework for controlling access rights to digital content in a distributed information system, comprising first storage means (table 220) for storing a reference to a user registered in the framework, second storage means (table 222) for storing a reference to digital content registered for the user, and third storage means (table 224) for storing a reference to a digital secure repository (rights wallet 204) registered for the user, the digital secure repository containing storage means for storing a unique identifier (rights wallet ID 230) and a reference (rights wallet list 232) to the digital content. Finally as recited in claim 1, the digital secure repository is associated with the user independently of a particular user device and stores access rights to the digital content granted to the user by a provider.

Claim 2, dependent on claim 1, recites the further presence of fourth storage means (table 226) for storing a reference to a rendering device (206) registered for the user. Claims 3-5 and 7-10 are also dependent on claim 1.

Claims 1-10 stand rejected as being unpatentable over Okamoto et al. U.S. Patent 6,732,106 ("Okamoto") in view of Fung et al. U.S. Patent Application Publication 2001/0052077 ("Fung") (page 2, ¶ 3).

Okamoto describes a digital data distribution system in which a distribution server 1001 (Fig. 10) distributes digital content to a user device 1002. At the distribution server 1001, a user administration database 1004 stores user account information (user ID, password, etc.) in a user account information database (Fig. 13), user device information (device ID, owner's user ID, etc.) in a user device information database (Fig. 14), and storage media information (media ID, recipient's user ID, etc.) in a storage media information database (Fig. 15) (col. 10, lines 12-35). Additionally at the distribution server 1001, an obtained rights administration database 1006 (Fig. 18) stores an indication of the rights obtained by various users (col. 10, lines 53-60), while a history database 1007 (Fig. 19) stores historical information on previous distributions to users (col. 10, lines 61-67).

When a user in the Okamoto system downloads content, he does so to a specific device 1002 (step S2612; col. 14, lines 64-65). If a user wishes to transfer the content to a different storage medium, he must revisit the distribution server and is limited in the number of times he can transfer to a different medium (Fig. 27; col. 15, lines 21-47). If a user wishes to transfer content to another device, he must begin the download process anew for that device. The user is thus tightly bound, not only to a particular device 1002, but also to the distribution server 1001 on which the rights information resides.

Okamoto presents his system, with its centralized maintenance of usage rights information and history information, as an improvement over a previous system (Fig. 32) in which such information is stored locally in a storage means 3212. Even if such locally stored information is regarded as a digital repository, such repository is bound with a particular device, namely the user device 3202. Indeed, Okamoto notes the difficulty in such a prior-art arrangement of transferring the digital rights to a different device should the first one fail (col. 2, lines 37-46). Clearly, then, the storage means 3212 is not associated with a user independently of a particular device as claimed by applicants.

Thus, Okamoto fails to teach having a digital secure repository that is associated with a user independently of a particular user device and stores access rights to digital content granted to the user by a provider. Therefore, this reference also fails to teach storing a reference to such a digital secure repository as claimed by applicants.

Fung describes a so-called universal mobile ID (UMID) system for digital rights management. In one embodiment (Fig. 2), each client 102 is associated with a UMID 200, which is locally stored. UMID 200 consists of a user ID (UID) 210 containing information relevant to a user and a device ID (DID) 220 containing information relevant to a particular device (¶ 8). Each client 102 also stores a secret PIN 213, which is used to decrypt locally stored content for rendering but is otherwise inaccessible to the user. Since this secret PIN 213 is necessary for rendering and is stored by the client 102 (¶ 54), the digital content is, in effect, bound to the device of the client 102. This is in addition to the binding created by the UMID 200 itself as a composite of the user ID 210 and device ID 220.

Although Fung's UID information is said to include "access rights" 122, those "access rights" relate to such things as blocking rights 122a for limiting the access of children to the Internet (¶ 31). Those "access rights" are thus more in the nature of parental controls, which are set by the user, and are not access rights granted to the user by a provider as claimed by applicants. In this sense, therefore, Fung contains no locally stored access rights information, and Fung is similar in Okamoto in that access rights are bound to a particular combination of user and device.

Thus, like Okamoto, Fung fails to teach having a digital secure repository that is associated with a user independently of a particular user device and stores access rights to digital content granted to the user by a provider. Therefore, this latter reference also fails to teach storing a reference to such a digital secure repository as claimed by applicants.

Claims 11-17

Claim 11 as amended is directed to a method for controlling access rights to digital content in a distributed information system. The method comprises the steps of registering a user with a framework for controlling access rights to digital content in the distributed information system, registering for the user a digital secure repository that is associated with the user independently of a particular user device and stores access rights to the digital content granted to the user by a provider, and registering digital content for the user. Claims 12-17 are dependent on claim 11.

Claims 11-13 and 15-17 stand similarly rejected as being unpatentable over Okamoto in view of Fung (page 2, ¶ 3), while claim 14 stands rejected on this combination of references together with the additional reference of Olson described below (pages 8-9, ¶ 4). As with claim 1, Fung is cited for its supposed teaching of a digital secure repository (page 6). However, as previously noted, the UMID 200 cited on this point does not store access rights granted to a user by a provider, nor is it associated with a user independently of a particular user device. Thus it does not constitute a digital repository such as claimed by applicants.

Claims 18-25

Claim 18 is directed to the rendering procedure shown in Figs. 8A-8B as it involves the rights wallet 204. More particularly, claim 18 as amended is directed to a method for rendering digital content on a rendering device in which, upon receiving a request for rendering digital content in a predetermined form (step 802), information about access rights granted to the digital content is read from a digital secure repository that is associated with a user independently of a particular user device and stores access rights to the digital content granted to the user by a provider (step 820). If the access rights cover the requested form of rendering the digital content, a document encryption key encrypted with a public key associated with the rendering device is obtained (steps 854-858) and decrypted with a private key associated with the rendering device (step 850). The digital content is then decrypted with the document encryption key (step 846) and rendered in the requested form (step 860). Claims 19-25 are dependent on claim 18.

Claims 18-25 stand rejected as being unpatentable over Okamoto in view of Fung and Olson et al. U.S. Patent Application Publication 2002/0003878 ("Olson") (pages 8-9, ¶ 4).

Okamoto and Fung have been discussed above. Olson describes a cryptographic key distribution system and method for digital video systems in which public key encryption system is used to encrypt video decryption keys so that they can be sent via a digital display link to an encryptor (¶ 54).

In rejecting claims 18-25 in their original form, the Examiner appears to rely on Okamoto for all of the recited steps except for the obtaining of the document encryption key in encrypted form and decrypting that key using a private key, for which Olson is cited (pages 10-11). Claim 18 as amended, however, recites that the information about access rights is read from a digital secure container of the type described above. Neither of the Okamoto and Fung references, however, teaches such a digital secure container. As recounted above, in Okamoto the storage for the access rights information is associated either with a server or with a specific user device. Similarly, in Fung, the access rights information is kept on a server, while the locally stored information relates to access rights granted <u>by</u> the user rather than access rights granted <u>to</u> the user as claimed by applicants.

In sum, none of the references cited by the Examiner teach the use of a digital secure repository of the type claimed by applicants. Accordingly, claims 18-25 distinguish patentably over the art cited by the Examiner.

Claims 26-27

Claims 26-27 are directed to the procedure shown in Fig. 9 for binding digital content to a rendering device. More particularly, claim 26 as amended is directed to a method in which a connection is established from the rendering device to a digital secure repository that is associated with a user independently of a particular user device and stores access rights of the user to the digital content (step 906). Access rights for specified digital content are requested from the digital secure repository (step 908). If binding is allowed according to the access rights stored in the digital secure repository, a respective document encryption key encrypted with a public key associated with the rendering device is received (step 922) and is stored for later decrypting the respective digital content (step 924). Claim 27 is drawn to a program storage device for practicing the method of claim 26.

Claims 26-27 stand rejected as being unpatentable over Okamoto in view of Fung and Olson (pages 8-9, ¶ 4). In reading the cited references ontò these claims (pages 13-15), the Examiner appears to rely on Okamoto for its alleged teaching of an interaction between two nodes to determine access rights (in this case binding rights), Fung for its alleged teaching of an interaction between a rendering device and a digital secure repository, and Olson for its alleged teaching of the usc of a public key associated with a rendering device. However, as the Examiner implicitly recognizes by using Fung as a secondary reference, the interaction that occurs in Okamoto to determine access rights is between a user device 1002 and a distribution server 1001, not between a rendering device and a digital secure repository associated with a user as claimed by applicants.

As for Fung, the interaction relating to access rights described in the cited paragraph 15 is between the client 102 and the server 120, not between a rendering device and a digital secure repository associated with a user as claimed by applicants. Moreover, the comparison does not improve even if wc look only at interactions within the client 102. Manifestly, the UMID 200 is not a digital secure repository of the type claimed by applicants, since it stores only access rights (such as blocking rights 122a) set by the user and does not store access rights granted to a user as claimed by applicants. Further, since the UMID 200 is a fusion of the user ID 210 and the device ID 220, it is not associated with a user independently of a particular user device as claimed by applicants. Thus, Fung's digital content is already "bound" to the user device. Indeed, the whole notion of determining whether binding "is allowed" in this scenario is nonsensical; it has already been done.

Finally, while Olson has been cited for its alleged disclosure of key-encrypting keys, applicants have never claimed this aspect per se as their invention.

To recapitulate, in terms of the language of claim 26 as amended, none of the references cited teaches a digital secure repository that is associated with a user independently of a particular user device and stores access rights of the user to digital content as claimed by applicants. Accordingly, claims 26 and 27 distinguish patentably over the art cited by the Examiner.

Claims 28-29

Claims 28-29 as amended are directed to the procedure shown in Fig. 10 for storing digital content from a rendering device onto a storage device. More particularly, claim 28 as amended is directed to a method for storing digital content from a rendering device onto a storage device in which a connection is established from the rendering device to a digital secure repository that is associated with a user independently of a particular user device and stores access rights of the user to the digital content (step 1006). Access rights for specified digital content are requested from the digital secure repository (step 1008). If storing is allowed according to access the rights stored in the digital secure repository, respective document encryption keys encrypted with respective public keys of all rendering devices registered in the digital secure repository are received (step 1020), and the encrypted keys are stored together with encrypted digital content on the storage device (steps 1022-1024). Claim 29 is drawn to a program storage device for practicing the method of claim 28.

Claims 28-29, like claims 26-27, stand rejected as being unpatentable over Okamoto in view of Fung and further in view of Olson (pages 8-9, ¶ 4). As with claims 26-27, in reading the cited references onto claims 28-29, the Examiner relies on Okamoto for its alleged teaching of an interaction between two nodes to determine access rights (in this case storage rights), Fung for its alleged teaching of an interaction between a rendering device and a digital secure repository, and Olson for its alleged teaching of the use of a public key associated with a rendering device (pages 15-17).

Here too, as the Examiner implicitly recognizes by using Fung as a secondary reference, the interaction in Okamoto is between a user device 1002 and a distribution server 1001, not between a rendering device and a digital secure repository associated with a user as claimed by applicant. As for Fung, the interaction described in paragraph 0015 is between the client 102 and the server 120, not between a rendering device and a digital secure repository associated with a user as claimed by applicants.

Thus, in terms of the language of claim 28 as amended, as with claim 26 as amended, none of the references cited teaches a digital secure repository that is associated with a user independently of a particular user device and stores access rights of the user to digital content as claimed by applicants. Accordingly, claims 28 and 29 likewise distinguish patentably over the art cited by the Examiner.

Claims 30-31

As already noted, these claims are directed to a method and computer program product for controlling the rendering of digital content to which a user has been granted access rights by a provider. As recited in these claims, the digital content is stored on a storage device accessible to a user, while the access rights to the digital content are stored in a digital secure repository that is associated with the user independently of a particular user device. The rendering of the digital content on a rendering device is controlled in accordance with the access rights to the digital content stored in the digital secure repository.

Claims 30-31 are believed to distinguish patentably over the art cited for reasons similar to those urged above. None of the references cited by the Examiner teaches controlling rendering digital content in accordance with access rights stored in a digital secure repository that is associated with a user independently of a particular user device.

Conclusion

All of applicants' claims recite the use of digital secure repository that is associated with a user independently of a particular user device and stores access rights to the digital content granted to the user by a provider. None of the references cited by the Examiner teach such a digital secure repository. Accordingly, applicants' claims distinguish patentable over the art cited by the Examiner.

Reconsideration of the application as amended is respectfully requested. It is hoped that upon such consideration, the Examiner will hold all claims allowable and pass the case to issue at an early date. Such action is earnestly solicited.

Respectfully submitted,
GERD BREITER et al.

By

William A. Kinnaman, Jr.
Registration No. 27,650
Phone: (845) 433-1175
Fax: (845) 432-9601

WAK/wak